

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-143658

(43)Date of publication of application : 28.05.1999

(51)Int.Cl.

G06F 3/12

G06F 12/14

**G06F 13/00**

**G06F 15/00**

(21)Application number : 09-307314

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 10.11.1997

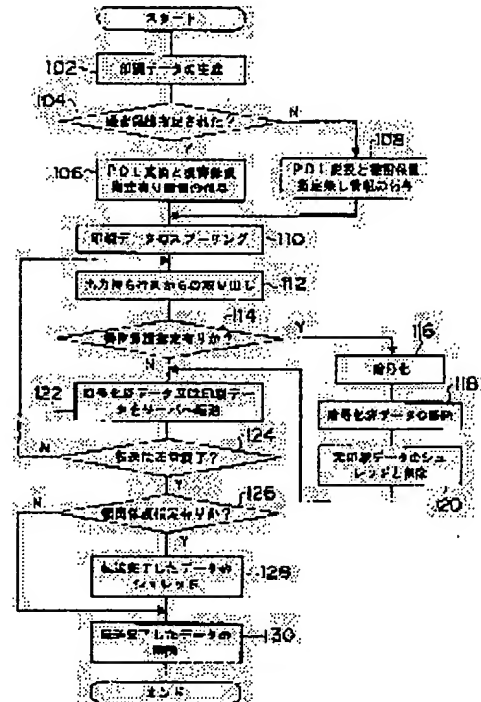
(72)Inventor : HIGO KAZUYOSHI

(54) NETWORK SYSTEM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent printing data being a security object from being referred to by the other person and from leaking to outside and to improve the security of printing data.

**SOLUTION:** In a client device, printing data of the security object which becomes unnecessary after transfer completes is electronically shredded (128) and printing data which becomes unnecessary after ciphering and which is in the state of pre-ciphering (120). Thus, secret is kept on printing data after transfer completes and printing data in the state of pre-ciphering. At the same time, a printing server and a printer electronically shred printing data being the security object, which becomes unnecessary after transfer and printing complete and decoded printing data which remains when transfer and printing abnormally terminate so as to keep secret.



## LEGAL STATUS

[Date of request for examination] 07.06.1999

[Date of sending the examiner's decision of rejection] 13.08.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3379411

[Date of registration] 13.12.2002

[Number of appeal against examiner's decision of rejection] 2002-17566

[Date of requesting appeal against examiner's decision of rejection] 12.09.2002

[Date of extinction of right]

(51) Int.Cl.<sup>6</sup>

識別記号

F I

G 0 6 F 3/12

G 0 6 F 3/12

C

12/14

3 2 0

12/14

3 2 0 D

13/00

3 5 1

13/00

3 5 1 A

15/00

3 3 0

15/00

3 3 0 A

審査請求 未請求 請求項の数5 OL (全 12 頁)

(21) 出願番号

特願平9-307314

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(22) 出願日

平成9年(1997)11月10日

(72) 発明者 肥後 和敬

埼玉県岩槻市府内3丁目7番1号 富士ゼ

ロックス株式会社岩槻事業所内

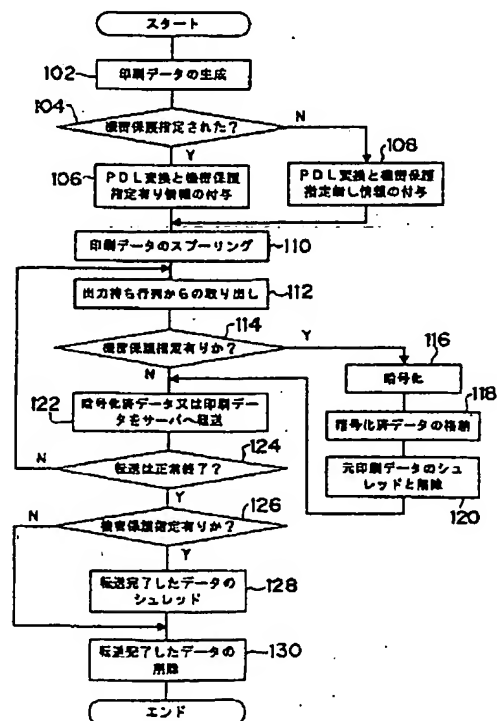
(74) 代理人 弁理士 中島 淳 (外3名)

(54) 【発明の名称】 ネットワークシステム

(57) 【要約】

【課題】 機密保護対象の印刷データが他者により参照され外部へ漏洩することを防ぎ、印刷データの機密保護性を向上させる。

【解決手段】 クライアント装置においては、転送完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする(128)と共に、暗号化後に不要となった暗号化前の状態の印刷データを電子的にシュレッドする(120)ので、転送完了後の印刷データ及び暗号化前の状態の印刷データについて機密が保持される。これと同様に、プリントサーバ及びプリンタの各々でも、転送や印刷の完了後に不要になった機密保護対象の印刷データ、及び転送や印刷の異常終了時に残存した復号された印刷データを電子的にシュレッドして、機密を保持する。



## 【特許請求の範囲】

【請求項1】 ネットワークを介して互いに接続されたクライアント装置、プリントサーバ及びプリンタを含んで構成され、前記クライアント装置から転送された印刷データが前記プリントサーバで一旦受信された後プリンタへ転送され、又は前記クライアント装置からの印刷データが前記プリンタへ直接転送され、該プリンタが受信した印刷データを印刷するネットワークシステムであって、

前記クライアント装置は、

機密保護対象とする印刷データを指定するための機密保護指定手段と、

前記機密保護指定手段により機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する情報付加手段と、

前記属性情報付加手段により機密属性情報が付加された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第1の加工手段と、

を有し、

前記プリンタ及び前記プリントサーバの各々は、

受信した印刷データに機密属性情報が付加されているか否かを判定する判定手段と、

前記判定手段により機密属性情報が付加されていると判定された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第2の加工手段と、

を有するネットワークシステム。

【請求項2】 前記第1の加工手段及び前記第2の加工手段の少なくとも一方は、前記機密属性情報が付加された印刷データの転送完了後又は印刷完了後に、該印刷データを判読不能なデータに加工することを特徴とする請求項1記載のネットワークシステム。

【請求項3】 前記クライアント装置は、

前記印刷データを暗号化する暗号化手段をさらに有し、前記第1の加工手段は、前記暗号化手段による印刷データの暗号化が行われた後、暗号化前の状態で残存した印刷データを判読不能なデータに加工し、

前記プリンタ及び前記プリントサーバの少なくとも一方は、前記暗号化手段により暗号化された印刷データを復号する復号化手段をさらに有し、

前記第2の加工手段は、前記復号化手段により復号された印刷データの転送完了後又は印刷完了後に、該復号された印刷データを判読不能なデータに加工する、

ことを特徴とする請求項1記載のネットワークシステム。

【請求項4】 前記第1の加工手段及び前記第2の加工手段の少なくとも一方は、前記機密属性情報が付加された印刷データの削除が指示された場合に、該印刷データを判読不能なデータに加工することを特徴とする請求項1記載のネットワークシステム。

【請求項5】 端末装置及び前記端末装置から転送され

てきた印刷データを印刷するプリンタを含んで構成されたネットワークシステムであって、

前記端末装置は、

機密保護対象とする印刷データを指定するための機密保護指定手段と、

前記機密保護指定手段により機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する情報付加手段と、

前記属性情報付加手段により機密属性情報が付加された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第1の加工手段と、

を有し、

前記プリンタは、

受信した印刷データに機密属性情報が付加されているか否かを判定する判定手段と、

前記判定手段により機密属性情報が付加されていると判定された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第2の加工手段と、

を有するネットワークシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、ネットワークシステムに係り、より詳しくは、クライアント装置又は端末装置からの印刷データを、ネットワークを介してプリンタへ転送し、プリンタで該印刷データを印刷するネットワークシステムに関する。

## 【0002】

【従来の技術】従来より、プリントシステムにおける機密保護方式として、印刷データ送信元であるクライアント装置が、該印刷データの取り出しを許可するパスワード情報を印刷データに付与してプリンタあるいはプリントサーバへ転送し、プリンタあるいはプリントサーバが、受信した印刷ジョブを一旦保留・保管した後、操作者から正規のパスワード（＝印刷データに付与されたパスワード情報に合致するパスワード）が入力された場合に印刷データをメモリから取り出し、印刷データの参照や印刷を実行する技術が知られている（特開平8-314659号公報参照）。

【0003】ところが、上記の技術は、プリンタあるいはプリントサーバにおいて、印刷データの取り出しが、正規のパスワードが入力されるまで抑止されるというだけであり、何ら暗号化等が施されていない印刷データが伝送路上を流れるという点で機密保護方式としては不十分であった。

【0004】これを改善するものとして、送信元であるクライアント装置が印刷データを暗号化し、暗号化された印刷データをプリンタあるいはプリントサーバへ転送し、これを受信したプリンタあるいはプリントサーバが復号して印刷データの参照や印刷を実現する技術が提案されている。この方式では、暗号化された印刷データを

10

20

30

40

50

伝送路上に流すことにより、伝送路上での印刷データの漏洩・判読を防止している。

【0005】このような暗号化技術と上記特開平 8-314659 号公報記載の技術とを併せて利用することにより、機密保護性はかなり高まったといえる。

【0006】しかしながら、これらの機密保護方式においては、暗号化や復号化を行った後に不要となった印刷データの機密保護については考慮されておらず、この不要となった印刷データがクライアント装置、プリンタ、プリントサーバの各々に内蔵された記憶装置（例えば、磁気ディスク装置等）に判読可能な状態で放置されてしまう。

【0007】即ち、通常利用される OS (Real Time Monitor 等も含む Operating System) 提供のファイルシステムでは、データの削除は、例えばファイルコントロールブロック内の削除ビットをオンにする等のデータ管理情報の変更操作による見かけ上での削除にすぎず、実際に削除対象のデータが NULL データ (X' 00') でクリアされる等の処理が施されるわけではない。

【0008】したがって、暗号化前の印刷データ及び復号化後の印刷データの中身は、他のファイルの新規作成や更新等の保存処理によりその記憶領域が他のデータで上書きされるまで、削除前と同じ状態で記憶装置上に存在し続けることとなる。

【0009】このため、通常用いられるファイル復旧ツールやディスクダンプツール等を利用すれば、機密保護対象の印刷データであっても参照できてしまう、といった問題があった。

【0010】

【発明が解決しようとする課題】本発明は、上記問題点を解消するために成されたものであり、機密保護対象の印刷データが他者により参照され外部へ漏洩することを防ぎ、印刷データの機密保護性を向上させることができるネットワークシステムを提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するために、本発明に係るネットワークシステムは、ネットワークを介して互いに接続されたクライアント装置、プリントサーバ及びプリンタを含んで構成され、前記クライアント装置から転送された印刷データが前記プリントサーバで一旦受信された後プリンタへ転送され、又は前記クライアント装置からの印刷データが前記プリンタへ直接転送され、該プリンタが受信した印刷データを印刷するネットワークシステムであって、前記クライアント装置は、機密保護対象とする印刷データを指定するための機密保護指定手段と、前記機密保護指定手段により機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する情報付加手段と、前記属性情報付加手段により機密属性情報が付加された印刷データを、該印刷データが不要となった時点で判読不能な

データに加工する第 1 の加工手段と、を有し、前記プリンタ及び前記プリントサーバの各々は、受信した印刷データに機密属性情報が付加されているか否かを判定する判定手段と、前記判定手段により機密属性情報が付加されていると判定された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第 2 の加工手段と、を有することを特徴とする。

【0012】本発明に係るネットワークシステムは、ネットワークを介して互いに接続されたクライアント装置、プリンタ及びプリントサーバを含んで構成されている。クライアント装置から転送された印刷データは、プリントサーバで一旦受信された後プリンタへ転送されるか、又はプリンタへ直接転送され、該プリンタにより印刷される。

【0013】このようなネットワークシステムにおいて、クライアント装置のユーザが機密保護指定手段により、機密保護対象とする印刷データを指定すると、情報付加手段は、該機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する。この機密属性情報としては、例えば、1 ビットで構成されるフラグ（機密保護対象の場合「1」、機密保護対象でない場合「0」など）を用いることができる。

【0014】この機密属性情報が付加された印刷データは、前述したように、プリントサーバで一旦受信された後プリンタへ転送されるか又はプリンタへ直接転送されるが、該印刷データが不要となった時点（例えば、該印刷データの転送完了後や、印刷取消しや印刷データの転送取消し等により印刷データの削除がユーザにより指示されたとき等）で、第 1 の加工手段により判読不能なデータに加工される。

【0015】なお、判読不能なデータへの加工方法としては、NULL データによるクリア、乱数によるスクランブル、各種の暗号化等を採用することができる。

【0016】これにより、クライアント装置において、不要となった機密保護対象の印刷データが該クライアント装置内のメモリに判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【0017】プリントサーバは上記機密属性情報が付加された印刷データを一旦受信した後、プリンタへ転送するが、このプリントサーバにおいて、判定手段が、受信した印刷データに機密属性情報が付加されているか否かを判定する。そして、第 2 の加工手段は、この判定結果により機密属性情報が付加されていると判定された印刷データ（即ち、機密保護対象として指定された印刷データ）を、該印刷データが不要となった時点（例えば、プリンタへの該印刷データの転送完了後や、印刷取消しや印刷データの転送取消し等により印刷データの削除がユーザにより指示されたとき等）で判読不能なデータに加工する。

【0043】ここで、印刷データが機密保護指定されていなければ、後述するステップ122へ進み、印刷データが機密保護指定されておれば、ステップ116へ進む。このステップ116では、暗号化制御部17によって印刷データの暗号化を行い、次のステップ118で暗号化済の印刷データを、スプーリング制御部15によって記憶装置18に格納する。さらに、次のステップ120では、暗号化によって不要となった暗号化前の印刷データを電子的にシュレッドした後削除する。

【0044】次のステップ122では、暗号化済の印刷データ又は機密保護指定されていない印刷データを、伝送制御部12の制御に基づいて、伝送I/F11を経由してプリントサーバ20へ転送する。

【0045】ここでの転送が何らかの理由により正常に完了しなかった場合、スプーリング制御部15によって印刷データは記憶装置18に保持される。そして、ステップ112へ戻り、ステップ112～122の処理を再実行する。

【0046】一方、ステップ122での転送が正常終了した場合は、ステップ126へ進み、不要となった転送済の印刷データが機密保護指定されているか否かを、該印刷データに付与された属性情報に基づいて判定する。

【0047】ここで、印刷データが機密保護指定されていなければ、該印刷データの削除のみを行う（ステップ130）。一方、印刷データが機密保護指定されている場合には、該印刷データをデータ加工部19によって電子的にシュレッドした（ステップ128）後、削除する（ステップ130）。

【0048】以上のように、クライアント装置10においては、転送完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする（図2のステップ128）ので、転送完了後の印刷データについて機密が保持される。また、暗号化後に不要となった暗号化前の状態の印刷データを電子的にシュレッドする（図2のステップ120）ので、暗号化前の状態の印刷データについて機密が保持される。

【0049】プリントサーバ20においては図3の制御ルーチンが実行される。図3のステップ202では、伝送制御部22の制御に基づいて、クライアント装置10からの属性情報付きの印刷データ（即ち、暗号化済の印刷データ又は機密保護指定されていない印刷データ）を受信し、次のステップ204では受信した印刷データをスプーリング制御部24によって記憶装置26に格納する。

【0050】そして、次のステップ206では、目的とするプリンタ30がデータの受け入れ準備可能であるか否かをプリンタ管理部29によって判定する。ここで、プリンタ30がデータの受け入れ準備可能と判定された時点で、ステップ208へ進み、属性情報付きの印刷データをスプーリング制御部24の待ち行列制御に従って

記憶装置26から取り出す。

【0051】次のステップ210では、印刷データが機密保護指定されているか否かを、該印刷データに付与された属性情報に基づいて判定する。ここで、印刷データが機密保護指定されていなければ、後述するステップ216へ進み、印刷データが機密保護指定されている場合は、ステップ212へ進む。ステップ212では、プリンタ30が復号機能を持っているか否かをプリンタ管理部29によって判定し、プリンタ30が復号機能を持っていない場合のみ、ステップ214へ進み、復号化制御部25によって各種暗号化に対応した復号処理を印刷データに対し実行し、復号された印刷データ（復号化済の印刷データ）を記憶装置26に格納する。

【0052】次のステップ216では、ステップ214で得られた復号化済の印刷データ又は機密保護指定されていない印刷データを、伝送制御部22の制御に基づいて伝送I/F21を経由してプリンタ装置30へ転送する。

【0053】ここでの転送が何らかの理由により正常に完了しなかった場合、スプーリング制御部24によって印刷データは記憶装置26に保持されるが、ステップ220で、該印刷データが機密保護指定されているか否かを判定部27によって判定し、機密保護指定されている場合のみステップ222へ進み、該印刷データ（ここでは復号化済の印刷データ）をデータ加工部28によって電子的にシュレッドして削除する。

【0054】その後、ステップ208へ戻り、ステップ208～216の処理を再実行する。

【0055】一方、ステップ216での転送が正常終了した場合は、ステップ224へ進み、不要となった転送済の印刷データが機密保護指定されているか否かを判定部27によって判定する。

【0056】ここで、印刷データが機密保護指定されていなければ、該印刷データの削除のみを行う（ステップ228）。一方、印刷データが機密保護指定されている場合には、該印刷データをデータ加工部28によって電子的にシュレッドした（ステップ226）後、削除する（ステップ228）。

【0057】以上のように、プリントサーバ20においては、転送完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする（図3のステップ226）ので、転送完了後の印刷データについて機密が保持される。また、転送が正常に完了しなかった場合、復号された機密保護対象の印刷データを電子的にシュレッドする（図3のステップ222）ので、復号された状態の印刷データについて機密が保持される。

【0058】プリンタ30においては図4の制御ルーチンが実行される。図4のステップ302では、伝送制御部32によって、プリントサーバ20からの属性情報付きの印刷データ（即ち、暗号化済の印刷データ、復号化

済の印刷データ、機密保護指定されていない印刷データの何れか)を受信し、次のステップ304では受信した印刷データをスプーリング制御部35の制御に基づいて記憶装置39に格納する。

【0059】そして、次のステップ306では、転写部38が転写可能状態となったか否かを判定する。ここで、転写部38が転写可能状態となった時点で、ステップ308へ進み、属性情報付きの印刷データをスプーリング制御部35の待ち行列制御に従って記憶装置39から取り出す。

【0060】次のステップ310では、印刷データが機密保護指定されているか否かを、該印刷データに付与された属性情報に基づいて判定する。ここで、印刷データが機密保護指定されていないければ、後述するステップ316へ進み、印刷データが機密保護指定されている場合は、ステップ312へ進む。ステップ312では、該印刷データが暗号化された状態の印刷データ(即ち、暗号化済の印刷データ)であるか否かを判定し、該印刷データが暗号化された状態の印刷データである場合のみ、ステップ314へ進み、復号化制御部34によって各種暗号化に対応した復号処理を印刷データに対し実行し、復号された印刷データ(復号化済の印刷データ)を記憶装置39に格納する。

【0061】次のステップ316では、上記復号された印刷データ、プリントサーバ20で既に復号されていた印刷データ、機密保護指定されていない印刷データに対して、ラスタイザ36によりラスタイズ処理が施され、ラスタイメージに展開される。そして、次のステップ318では、該ラスタイメージを印刷制御部37の制御に基づいて転写部38に転送し用紙に転写することで、印刷処理を行う。

【0062】ここでの印刷処理が何らかの理由により正常に終了しなかった場合、スプーリング制御部35の制御によって印刷データは記憶装置39に保持されるが、ステップ322で、該印刷データが機密保護指定されているか否かを判定部3Aによって判定し、機密保護指定されている場合のみステップ324へ進み、該印刷データ(ここでは復号化済の印刷データ)をデータ加工部3Bによって電子的にシュレッドして削除する。

【0063】その後、ステップ308へ戻り、ステップ308~318の処理を再実行する。

【0064】一方、ステップ318での印刷処理が正常終了した場合は、ステップ326へ進み、不要となった印刷済の印刷データが機密保護指定されているか否かを判定部3Aによって判定する。

【0065】ここで、印刷データが機密保護指定されていないければ、該印刷データの削除のみを行う(ステップ330)。一方、印刷データが機密保護指定されている場合には、該印刷データをデータ加工部3Bによって電子的にシュレッドした(ステップ328)後、削除する

(ステップ330)。

【0066】以上のように、プリンタ30においては、印刷完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする(図4のステップ328)ので、印刷完了後の印刷データについて機密が保持される。また、印刷が正常に完了しなかった場合、復号された機密保護対象の印刷データを電子的にシュレッドする(図4のステップ324)ので、復号された状態の印刷データについて機密が保持される。

【0067】ところで、クライアント装置10のユーザは、前述した図2の制御ルーチンの任意の処理時点で、印刷処理の取消しや転送の取消しといった印刷データを削除する指示をクライアント装置10に対して操作制御部16を通じて指示可能である。即ち、クライアント装置10のユーザにより印刷データの削除指示が行われると、クライアント装置10において図5の処理ルーチンが割り込み処理される。まず、印刷データの削除指示を受け取ったスプーリング制御部15は、該印刷データが機密保護指定されているか否かをチェックし(ステップ402)、機密保護指定されていないければ、該印刷データの削除のみを行う(ステップ406)。一方、印刷データが機密保護指定されている場合は、該印刷データをデータ加工部19によって電子的にシュレッドして(ステップ404)、削除する(ステップ406)。

【0068】このように、機密保護指定された印刷データに対して削除指示が行われた(印刷の取消しや転送の取消しが指示された)場合、該印刷データは直ちに電子的にシュレッドされるので、不要となった機密保護対象の印刷データが記憶装置18に判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【0069】なお、上記のような機密保護指定の印刷データに対する削除指示時の割り込み処理(図5)は、クライアント装置10だけでなく、プリントサーバ20及びプリンタ30においても実行される。即ち、プリントサーバ20のユーザが、印刷処理の取消しや転送の取消しといった印刷データ削除指示を、操作制御部23を通じて行えば、図5の処理ルーチンが割り込み処理され、機密保護対象の印刷データについてはデータ加工部28によって直ちに電子的にシュレッドされる。また、プリンタ30のユーザが、印刷処理の取消しや転送の取消しといった印刷データ削除指示を、操作制御部33を通じて行えば、図5の処理ルーチンが割り込み処理され、機密保護対象の印刷データについてはデータ加工部3Bによって直ちに電子的にシュレッドされる。

【0070】このようにして、プリントサーバ20やプリンタ30においても、不要となった機密保護対象の印刷データが記憶装置に判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【0071】以上説明した実施形態によれば、クライアント装置10のアプリケーション13が印刷データを生成してから、プリンタ30が該印刷データを印刷完了するまでの一連の印刷処理に関わるクライアント装置10、プリントサーバ20、プリンタ30の各々において、機密保護指定の印刷データは不要になった時点で直ちに電子的にシュレッドされるので、意図しない他者により印刷データが参照される可能性がなくなるため、印刷システムとして一貫した機密保護を保つことができる。

【0072】なお、本実施形態においては、プリントサーバ20に復号化制御部25を設けているが、この復号化制御部25は、プリンタ30が旧来のプリンタのように復号化機構を備えていない場合にのみ必要となるものである。プリントサーバ20の復号化制御部25によって、暗号化された印刷データを復号し、復号された印刷データを、伝送媒体41を介してプリンタ30へ転送する場合、判読可能な印刷データが伝送媒体41を流れてしまうため、機密保護上は本来望ましくないものである。但し、実際の利用現場では、様々な仕様を有する各種のプリンタを混在利用するケースが多いと想定されるため、上記実施形態では、プリントサーバ20に復号化制御部25を設け、復号化機構を備えていないプリンタから印刷データを印刷する場合でも対応可能な構成例を説明した。

【0073】また、上記実施形態では、クライアント装置10で生成した印刷データを、プリントサーバ20を経由してプリンタ30へ転送して印刷する処理形態に本発明を適用した例を示したが、クライアント装置10からプリントサーバ20に対し印刷要求のみを行い、印刷データについてはクライアント装置10からプリンタ30へ直接転送して印刷する処理形態についても、本発明は適用可能である。もちろん、図6に示すように端末装置70とプリンタ80とがローカル接続されたネットワークシステム90についても、本発明が適用可能であることは言うまでもない。

【0074】また、印刷データを暗号化した状態で装置間を転送しない場合でも、クライアント装置やプリントサーバでは転送完了後に、プリンタでは印刷完了後に不要となった印刷データを電子的にシュレッドすることにより、印刷データの機密性向上が図れる。また、ユーザ

により印刷データの削除指示が行われた時に、直ちに印刷データを電子的にシュレッドすることにより、印刷データの機密性向上が図れる。

【0075】

【発明の効果】以上説明したように、本発明によれば、機密保護対象として指定された印刷データは、クライアント装置、サーバ及びプリンタの各々において、該印刷データが不要となった時点で、判読不能なデータに加工されるので、不要となった機密保護対象の印刷データが装置内のメモリに判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【図面の簡単な説明】

【図1】発明の実施形態におけるネットワークシステムの概略構成図である。

【図2】クライアント装置において実行される制御ルーチンを示す流れ図である。

【図3】プリントサーバにおいて実行される制御ルーチンを示す流れ図である。

【図4】プリンタにおいて実行される制御ルーチンを示す流れ図である。

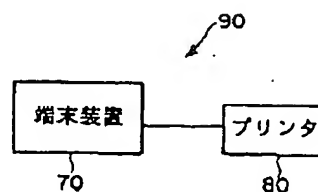
【図5】印刷データの削除指示により実行される割り込み処理ルーチンを示す流れ図である。

【図6】本発明を適用可能な他のネットワークシステムの概略構成図である。

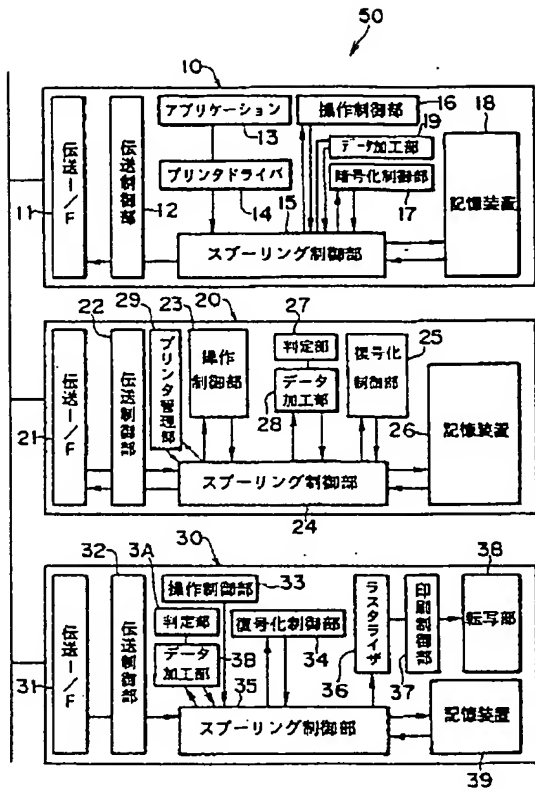
【符号の説明】

- 10 クライアント装置
- 15、24、35 スプーリング制御部
- 16 操作制御部（機密保護指定手段）
- 17 暗号化制御部（暗号化手段）
- 18、26、39 記憶装置
- 19 データ加工部（第1の加工手段、情報付加手段）
- 20 プリントサーバ
- 25、34 復号化制御部（復号化手段）
- 27、3A 判定部（判定手段）
- 28、3B データ加工部（第2の加工手段）
- 30 プリンタ
- 41 伝送媒体
- 50 ネットワークシステム

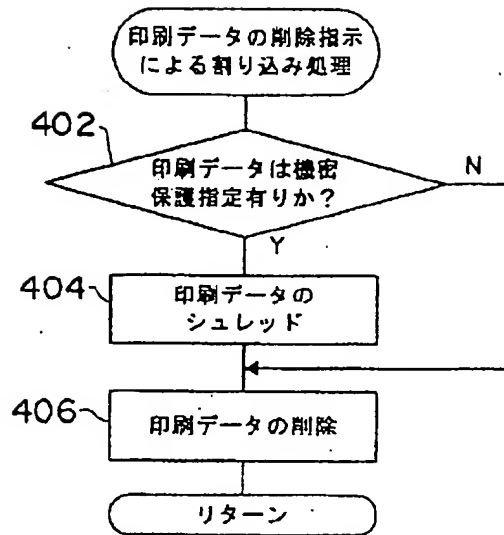
【図6】



【図1】

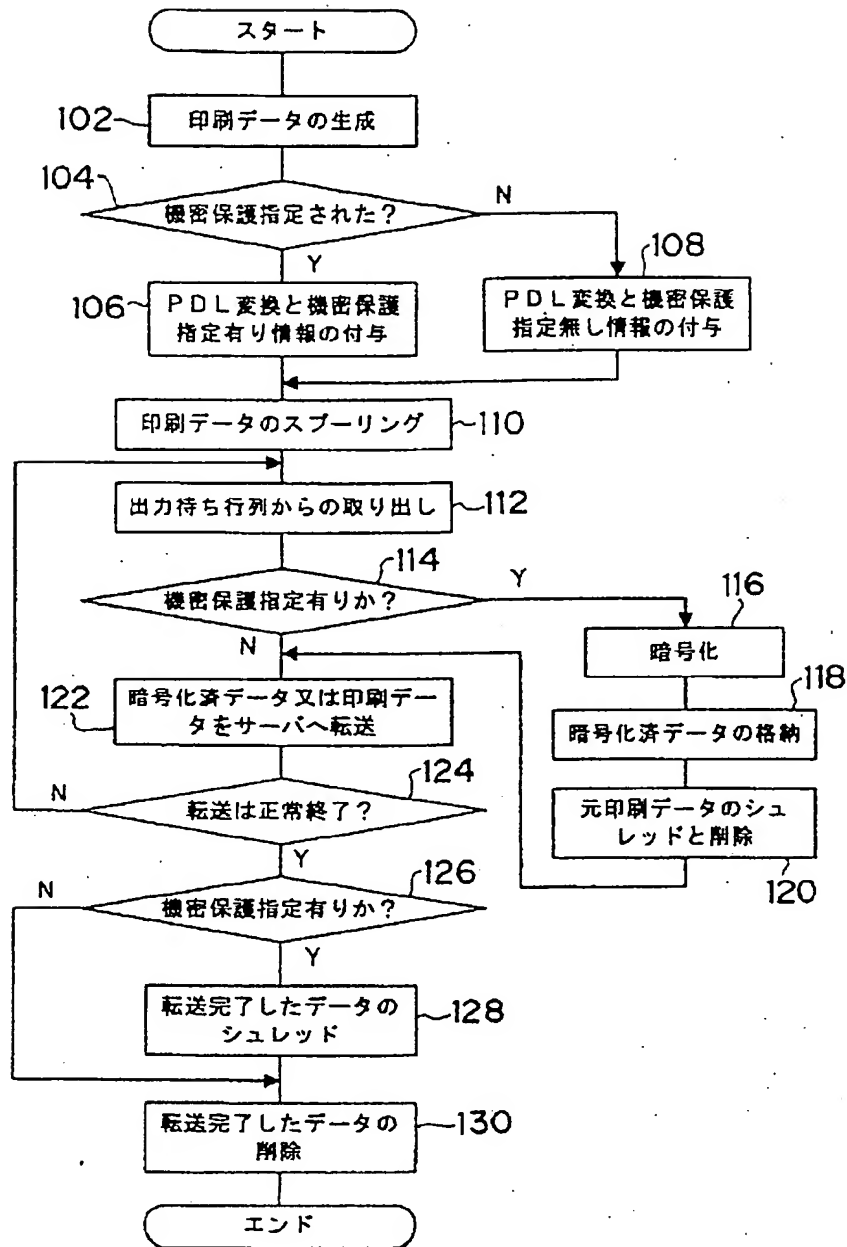


【図5】

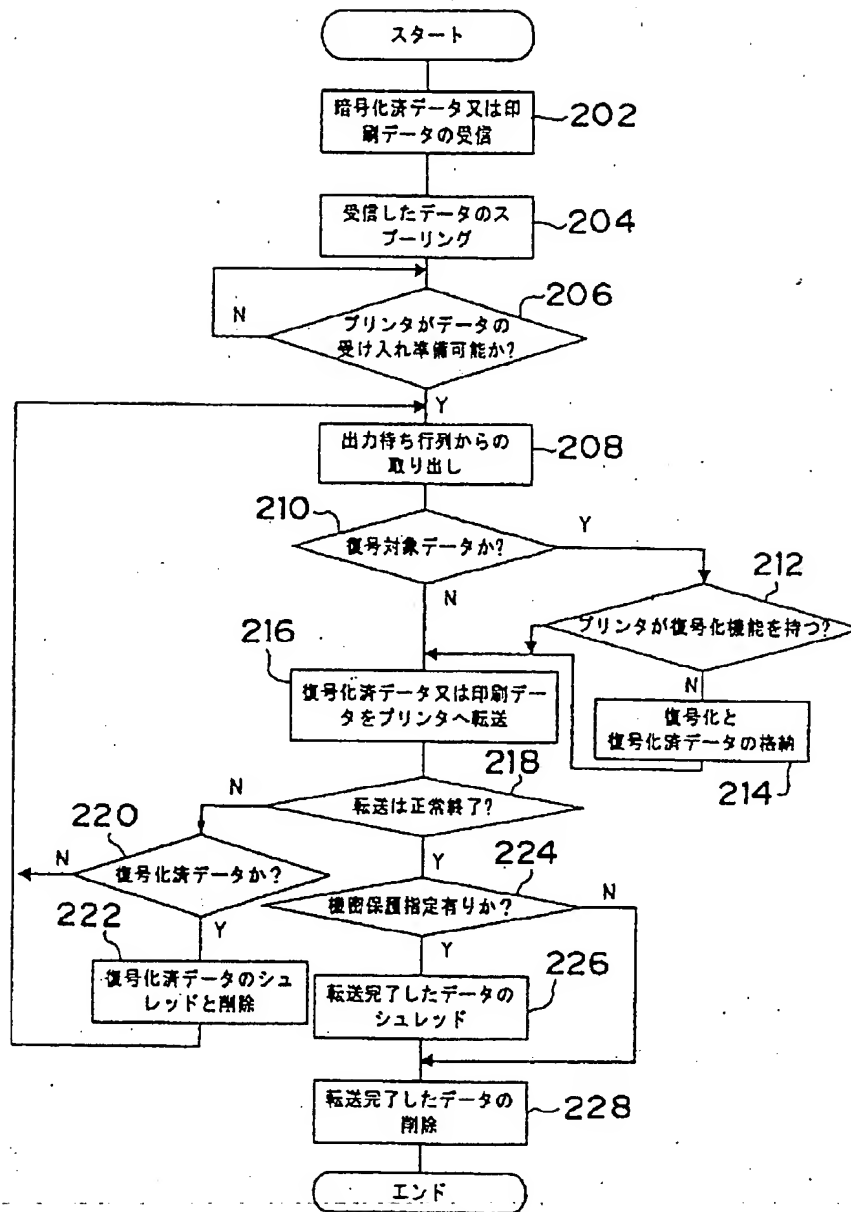




【図2】



【図3】



【図4】

